UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/836,965	04/17/2001	Alfred C. Shc	51040.P005	8500

43831 7590 11/27/2006

BERKELEY LAW & TECHNOLOGY GROUP
1700NW 167TH PLACE
SUITE 240
BEAVERTON, OR 97006

EXAMINER
TRUONG, THANHNGA B

ART UNIT	PAPER NUMBER
2135	

DATE MAILED: 11/27/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/836,965	SHE ET AL.	
	Examiner	Art Unit	
	Thanhnga B. Truong	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE ____ MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *05 September 2006*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-31* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☐ Claim(s) *1-3,10-12,20-23 and 31* is/are rejected.

7)☐ Claim(s) *4-9,13-19 and 24-30* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *17 April 2001* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Applicant's amendment filed on September 05, 2006 has been entered. Claims 1-31 are pending. Claims 1, 3-4, 12-13, 21-22, and 24 are amended by the applicant.

Claim Rejections - 35 USC § 103

2. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

3. Claims 1-3, 10-12, 20-23, and 31 are rejected under 35 U.S.C. 103(a) as being unpatentable over Wright (US 6,052,466), and further in view of Nakamura (US 5,159,633) and Coppersmith et al (US 6,192,129).

a. *Referring to claim 1:*

i. Wright teaches:

(1) generating in real time a first deciphering round key based on a deciphering key; incrementally deciphering a ciphered text for a first round using the real time generated first deciphering round key to generate a partially deciphered text (e.g., original plaintext); generating in real time a second deciphering round key based, at least in part, on said generated first deciphering round key while said incremental deciphering for said first round is being performed; and incrementally deciphering the partially deciphered text for a second round using the real time generated second deciphering round key **[i.e., reference is now made to Figure 4 wherein there is shown a flow diagram for secondary private key generation. For a bi-directional data communication between Party A and Party B as illustrated in Figure 3, the private key K actually comprises (i.e., may be split into) two keys K.sub.AB and K.sub.BA. The need for two private keys when handling bi-directional communications is required to ensure that the same cipher stream is never used for the encryption of different plaintext sequences. The first private**

key K.sub.AB is used to generate a forward first cipher stream C.sub.AB, and the second private key K.sub.BA is used to generate a reverse first cipher stream C.sub.BA. The forward first cipher stream C.sub.AB is then partitioned and indexed to generate a first (or forward channel) secondary private key C.sub.ABi sequence, with individual ones in the sequence used to generate a forward second cipher stream C.sub.AB ' that is used by security device 112A to encrypt Party A PT.sub.i data communications, and by security device 112B to decrypt Party A CT.sub.i data communications. The reverse first cipher stream C.sub.BA, on the other hand, is then partitioned and indexed to generate a second (or reverse channel) secondary private key C.sub.BAi sequence, with individual ones in the sequence used to generate a reverse second cipher stream C.sub.BA ' that is used by security device 112B to encrypt Party B PT.sub.i data communications, and by security device 112A to decrypt Party B CT.sub.i data communications (column 6, lines 22-45). In addition, in passive operation, no message exchange between Party A and Party B regarding synchronization is required as the index is merely passively incremented with each encryption or decryption and monitoring of the index field 148 (Figure 5) of each sent ciphertext sequence CT.sub.i (column 8, lines 22-26). Furthermore, Figure 8 describes more details in incrementing with each encryption or decryption process (column 8, lines 48-67 through column 9, lines 1-21 of Wright). Wright also further discloses generating/converting back to the original plaintext in column x, lines x-x.

ii. Although Wright is silent on the capability of the real time communication type information and how many rounds of cipher processing have been performed, Nakamura and Coppersmith teaches:

(1) in multimedia networks for transmitting real-time communication type information which must be encrypted in real time, and storage type information which requires safety-guaranteed encryption and certification of an information source via the same medium, Nakamura's invention is applicable to various other systems, and does not depend on network systems, and kinds of terminals **(column 12, lines 18-25 of Nakamura)**. In addition, encryption/decryption of real-time

communication type information by the secret-key system of this embodiment is described more in details in **column 6, lines 44-67 through column 7, lines 17 of Nakamura.**

(2) Referring to Figure 3, the first Step 100 is to initialize the iteration counter, "r", to keep track of how many rounds of cipher processing have been performed. At Step 110, a comparison is made between the iteration counter and the number of rounds of processing required. While the iteration counter is less than the number of rounds, the processing will continue on to Step 120. However, if the two values compared are equal, then encryption of the block has completed. It will be understood that the encryption process for each block of data forming the input file is identical, and that the process of Figure 3 is used on each successive block until all blocks of the input file have been encrypted **(column 7, lines 48-59 of Coppersmith).**

iii. It would have been obvious to a person having ordinary skill in the art at the time the invention was made to:

(1) have included the real-time communication type information in Wright so that the encrypted information cannot be easily decrypted **(column 2, lines 37-38 of Nakamura).**

(2) have included the number of rounds of cipher processing in Wright since the goal of a cipher is to be computationally infeasible to "break"--that is, it must be nearly impossible to "guess" or derive the original data content from any series of computations that can be performed on the transformed data, absent knowledge of how the encryption was accomplished **(column 1, lines 60-65 of Coppersmith).**

iv. The ordinary skilled person would have been motivated to:

(1) have included the real-time communication type information since when a secret-key for encrypting real-time communication type information is determined in advance, a communication is performed using the public-key cryptosystem used in encryption of storage type information, and the determined secret-key is abandoned after each communication. Thus, the secret-key for encrypting real-time communication type information can be prevented from being found out by a

third party, and high-speed information can be safely transmitted **(column 3, lines 16-24 of Nakamura).**

(2) have included the number of rounds of cipher processing because one way to make a cipher stronger is to increase the number of rounds of ciphering performed: with each successive transformation, the resulting encryption becomes more difficult to break. Another way to increase the strength is to increase the size of the key. Since the contents of the key remain secret, increasing the size adds another level of difficulty for anyone trying to deduce what transformations may have been performed on the original data, because they are unlikely to guess the random number combination making up the key **(column 2, lines 31-40 of Coppersmith).**

b. *Referring to claim 2:*

i. Wright further teaches:

(1) wherein said first and second deciphering round keys comprise first and second plurality of round key data words respectively, and said generation in real time of said second deciphering round keys comprises iteratively generating said second plurality of round key data words over a plurality of iterations **[i.e., each transmitted ciphertext data packet then includes an index identifying which of the plurality of secondary keys was used for the encryption (column 4, lines 15-19)].**

c. *Referring to claim 3:*

i. Wright further teaches:

(1) wherein said iterative generation of said second plurality of round key data words over a plurality of iterations comprises generating one of said second plurality of round key data words each iteration, including performance of a first XOR operation on a first and a second round key data word during each iteration **[i.e., referring to Figure 3, the encrypting/decrypting device 118 comprises a first cipher stream generator 120, a partitioning and indexing device 121, a second cipher stream generator 123 and an exclusive OR (XOR) multiplier 122 (column 5, lines 9-13)].**

f. *Referring to claims 10 and 21:*

i. These claims have limitations that is similar to those of claim 1, thus they are rejected with the same rationale applied against claim 1 above.

g. *Referring to claims 11 and 22:*

i. These claims have limitations that is similar to those of claim 2, thus they are rejected with the same rationale applied against claim 2 above.

h. *Referring to claims 12 and 23:*

i. These claims have limitations that is similar to those of claim 3, thus they are rejected with the same rationale applied against claim 3 above.

i. *Referring to claims 20 and 31:*

i. Wright, Nakamura, and Coppersmith teaches the claimed subject matter of deciphering round key generation. In addition, Nakamura further teaches:

(1) wherein said routing apparatus is disposed on an integrated circuit **[i.e., In Figures 7 and 8, reference numerals 71 and 81 denote these information equipments; 72 and 82, clock extraction circuits for extracting clock components from information signals; 73 and 83; pseudo random number generators; 74 and 84, control circuits for controlling synchronization of communications, generation of pseudo random numbers, automatic operations of the information equipments, and the like; 75 and 85, EX-OR gates for logically EX-ORing signals; and 76 and 86, transmission/reception circuits for transmitting/receiving signals onto/from transmission lines (column 11, lines 2737)].**

Response to Argument

4. Applicant's arguments filed September 05, 2006 have been fully considered but they are not persuasive.

Applicant argues that:

There is no teaching or remote suggestion in Wright concerning incremental deciphering. Incremental deciphering refers to an operation and/or process used in block encryption/decryption as opposed to stream encryption/decryption. It is to

be understood that incremental deciphering is the deciphering operation that takes place in a particular round of deciphering. The deciphering is incremental because a round key can only partially decipher the ciphered text block. Application of a multiplicity of round keys, each in its own particular round of deciphering, to the same text block in its successively partially deciphered state can ultimately produce the completely deciphered text block.

Examiner disagrees with the applicant and still maintains that:

Wright teaches a first cipher stream generated from a private key negotiated as a result of a public key exchange is partitioned to form a sequence of secondary keys. The secondary keys are then indexed. In one instance, each plaintext data packet is encrypted with a second cipher streams generated from a different one of the secondary keys. In another instance, a second cipher stream generated from a single secondary key is used to encrypt a plurality of plaintext data packets. A new second cipher stream generated from another one of the secondary keys is then used for encryption following each instance of the loss of a ciphertext data packet. The index is communicated with the ciphertext to identify which secondary key is to be used in generating the second cipher stream needed for decryption. With knowledge of the secondary key to be used, re-synchronization (along with new private key negotiation) at each instance of a ciphertext data packet loss is obviated (see abstract).

Although Wright's Figure 8 describes more details in incrementing with each encryption or decryption process **(column 8, lines 48-67 through column 9, lines 1-21),** Wright is silent on the capability of how many rounds of cipher processing have been performed. On the other hand, **Coppersmith teaches a method and apparatus for advanced byte-oriented symmetric key block cipher with variable length key and block *(emphasis added).*** Furthermore, referring to Figure 3, the first Step 100 is to initialize the iteration counter, "r", to keep track of how many rounds of cipher processing have been performed. At Step 110, a comparison is made between the iteration counter and the number of rounds of processing required. While the iteration counter is less than the number of rounds, the processing will continue on to Step 120. However, if the two values compared are equal, then encryption of the block

has completed. **It will be understood that the encryption process for each block of data forming the input file is identical, and that the process of Figure 3 is used on each successive block until all blocks of the input file have been encrypted *(emphasis added)* (column 7, lines 48-59 of Coppersmith).** In addition, Coppersmith further teaches, a commonly used cipher is known as the Data Encryption Algorithm ("DEA"). This algorithm was developed by scientists of the International Business Machines Corporation ("IBM"), and formed the basis of a United States federal standard known as the Data Encryption Standard ("DES"), which was adopted in 1977. DES has been in use since that time. A variant of the DES algorithm, known as "Triple DES", was developed to increase the strength of the result over that available with DES. Triple DES uses three rounds of ciphering, with different keys for each of the rounds *(emphasis added).* After twenty years, many believe that a new stronger, more flexible algorithm is needed. One way to make a cipher stronger is to increase the number of rounds *(emphasis added)* of ciphering performed: with each successive transformation, the resulting encryption becomes more difficult to break **(column 2, lines 20-34 of Coppersmith).** Furthermore, another object of the present invention is to provide a solution that allows precomputing the sub-keys to be used for each round of ciphering *(emphasis added)*, in order to minimize the time required for encrypting or decrypting an individual file or message. Still another object of the present invention is to provide a technique whereby the cipher used for encryption and decryption is block-oriented, uses a symmetric key, and uses different sub-keys during each round of ciphering. A further object of the present invention is to provide a technique whereby the cipher uses a variable number of rounds *(emphasis added)* of processing during encryption and decryption, a variable length block of data as the unit to be encrypted and decrypted, and a variable length key. Allowing these factors to vary will provide the user with choices that will not only affect execution time and strength of security for any given use of the cipher, but will also allow variation between subsequent uses of the cipher, further increasing the difficulty of breaking encrypted data from a given source **(column 3, lines 50-67 through column 4, line 1 of Coppersmith).**

In response to applicant's argument that there is no suggestion to combine the references, the examiner recognizes that obviousness can only be established by combining or modifying the teachings of the prior art to produce the claimed invention where there is some teaching, suggestion, or motivation to do so found either in the references themselves or in the knowledge generally available to one of ordinary skill in the art. See *In re Fine*, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988)and *In re Jones*, 958 F.2d 347, 21 USPQ2d 1941 (Fed. Cir. 1992). In this case, the combination of teaching between Wright, Nakumura, Coppersmith, and Adler is sufficient.

In response to applicant's argument that the references fail to show certain features of applicant's invention, it is noted that the features upon which applicant relies (i.e., Incremental deciphering refers to an operation and/or process used in block encryption/decryption; and the deciphering is incremental because a round key can only partially decipher the ciphered text block) are not recited in the rejected claim(s). Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

Thus, Wright, Nakumura, Coppersmith, and Adler do not need to disclose anything over and above the invention as claimed in order to render it unpatentable or anticipate. A recitation of the intended use of the claimed invention must result in a structural difference between the claimed invention and the prior art in order to patentably distinguish the claimed invention from the prior art. If the prior art structure is capable of performing the intended use, then it meets the claimed limitations.

For the above reasons, it is believed that the rejections should be sustained.

Allowable Subject Matter

5. Claims 4-9, 13-19, 24-30 objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

Conclusion

6. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Thanhnga (Tanya) Truong whose telephone number is 571-272-3858.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached at 571-272-3859. The fax and phone numbers for the organization where this application or proceeding is assigned is 571-272-8300.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 571-272-2100.

TBT
November 14, 2006

KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100